

POL-20081107A

STATEWIDE INFORMATION SECURITY POLICY

Information Security Identification And Authentication

Draft

Office of the Chief Information Officer

Department of Administration
Information Technology Services Division
PO Box 200113
Helena, MT 59620-0113
Tel: (406) 444-2700
FAX: (406) 444-2701

<*Date Published*>



Brian Schweitzer
Governor

State of Montana

DEPARTMENT OF ADMINISTRATION

Janet R. Kelly, Director

CHIEF INFORMATION OFFICER

Richard B. Clark

DRAFT STATEWIDE POLICY: INFORMATION SECURITY IDENTIFICATION AND AUTHENTICATION

EFFECTIVE DATE: DECEMBER 1, 2010

APPROVED: <DATE APPROVED>

I. Statement of Management Commitment

Threats to information systems today include environmental disruptions, human errors, and purposeful attacks by hostile entities such as nation states, terrorist groups, hackers, criminals, and disgruntled employees. Senior management understands their responsibilities in managing the risks from information systems that support the missions and business functions of the organization. Attacks on information systems today are often well organized, disciplined, aggressive, well funded, and in a growing number of documented cases, extremely sophisticated. Successful attacks on public and private sector information systems can result in unauthorized disclosure or modification of highly sensitive information or a mission impacting denial of service.

For risks related to identification and authentication, senior leadership recognizes that it is essential to make a fundamental commitment to make information security a first-order mission or business requirement.

II. Purpose

This **Information Security Identification And Authentication Policy** (Policy) establishes the requirements to implement Information Security Identification And Authentication standard(s) and associated procedures within agencies.

III. Authority

This instrument has been developed by the Office of the Chief Information Officer of the State of Montana to further the statutory responsibilities under [§2-17-534 MCA. Security responsibilities of department](#), as delegated by the Director, Department of Administration.

The State of Montana Chief Information Officer is responsible for developing policies, standards and guidelines, including minimum requirements, for providing adequate information security for agency operations and assets. This Policy is consistent with the requirements of the Montana Information Technology Act for securing information technology and [§2-15-114 MCA. Security responsibilities of departments for data](#).

This Policy has been prepared for use by State agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on agencies

under statutory authority. Nor should this Policy be interpreted as altering or superseding the existing authorities of the department directors or any other State official.

This Policy may conflict with other instruments currently in effect. Where conflicts exist, the more restrictive instrument governs. The development of future policies or standards will explicitly identify and retire any superseded portions of current policies or standards.

IV. Policy Statement

It is the policy of the State of Montana (State) that agencies shall develop and implement Identification And Authentication security controls on their information systems based upon (a) the [National Institute of Standards and Technology Guidance](#), and (b) the guidance articulated within the [Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies \(OMB 04-04\)](#).

V. Applicability

This Policy is applicable to agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), which have access to, or use or manage information assets subject to the policy and standard provisions of [§2-17-534, MCA](#). This Policy shall be communicated to staff and others who have access to or manage information and information systems and assets.

VI. Scope

The Policy authorizes and requires the implementation of an identification and authentication standard and associated procedures for the information systems and assets managed or controlled by agencies.

This Policy encompasses information systems for which agencies have administrative responsibility, including systems managed or hosted by third-parties on behalf of agencies.

This Policy may conflict with other information system policies currently in effect. Where conflicts exist, the more restrictive policy shall govern. The development of future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

VII. Definitions

Agency	Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA .
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.
Information Technology	Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA .

Refer to the [National Information Assurance \(IA\) Glossary](#), at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information assurance definitions.

Note: Because newer versions of the publications referenced herein become available from time-to-time, the latest publicly available versions at *the date of Policy approval* shall apply. However, each agency is encouraged to stay current by using the most recent versions. Future revisions of this Policy shall reference then currently-available versions.

VIII. Authorizations, Roles, and Responsibilities

Refer to the [Statewide Guidelines: Information Systems Security, paragraph II Authorizations, Roles, & Responsibilities](#) for applicable authorization, roles, and responsibilities.

IX. Requirements

Each agency shall:

1. Implement this Policy and its associated standard(s) in compliance with, and integrated with guidance provided by the [National Institute of Standards and Technology Guidance](#), and (b) the guidance articulated within the [Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies \(OMB 04-04\)](#).
2. Establish a framework of standards and procedures to initiate, control and evaluate the implementation of Identification And Authentication security controls.
3. Establish and evaluate performance measures to assess implementation of this Policy and subordinate standard(s) and procedures.

X. Compliance

Compliance with this Policy shall be evidenced by implementation of the Statewide Standard: Information Security Identification And Authentication.

XI. Policy Changes and Exceptions

Policy changes or exceptions are governed by the [Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards](#). Requests for a review or change to this instrument are made by submitting an [Action Request](#) form (at

http://itsd.mt.gov/policy/policies/action_request.doc). Requests for exceptions are made by submitting an [Exception Request](#) form (at http://itsd.mt.gov/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

XII. Closing

Direct questions or comments about this instrument to the State of Montana Chief Information Officer at [ITSD Service Desk](#) (at <http://servicedesk.mt.gov/ess.do>), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

XIII. References

A. Legislation

- [§2-15-114 MCA](#) – Security Responsibilities of Departments for Data.
- [§2-17-534 MCA](#) - Security Responsibilities of Department.

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- [MOM 3-0130 Discipline](#)
- Statewide Policy: Computer Security Incident Management
- State of Montana Continuity of Government plans, policies, standards, and procedures (future)
- [Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards](#)
- [Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards](#)

C. Standards, Guidelines

- [Guide To NIST Information Security Documents](#)
- [Office of Management and Budget Memorandum E-Authentication Guidance for Federal Agencies \(OMB 04-04\), Attachment A](#)
- [NIST SP800-53 Recommended Security Controls for Federal Information Systems](#)
- [NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 1, Low-Impact Baseline Identification and Authentication \(IA\) family \(Annex 1\)](#)
- [NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 2, Moderate-Impact Baseline Identification and Authentication \(IA\) family](#)

- [NIST SP800-53 Recommended Security Controls for Federal Information Systems, Annex 3, High-Impact Baseline Identification and Authentication \(IA\) family](#)
- [NIST SP800-39 Managing Risk from Information Systems – An Organizational Perspective](#)
- [NIST SP800-63 Revision 1 Electronic Authentication Guideline](#)
- [FIPS Pub 201-1 Personal Identity Verification \(PIV\) of Federal Employees and Contractors.](#)
- [FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems](#)
- [FIPS PUB 190 Guideline For The Use Of Advanced Authentication Technology Alternatives](#)
- [NIST SP800-60 Guide for Mapping Types of Information and Information Systems to Security Categories](#)

DRAFT

XIV. Administrative Use

Product ID: POL-20081107a
Proponent: Chief Information Officer
Publisher: Office of the Chief Information Officer
Published Date: <Date Published>
Version: 0.5.11
Version Date: 3/2/2009
Custodian: Policy Manager
Approved Date: <Date Approved>
Effective Date: December 1, 2010
RIM Class: Record
Disposition Instructions: Retain for Record
Change & Review: [ITSD Service Desk](http://servicedesk.mt.gov/ess.do) (at <http://servicedesk.mt.gov/ess.do>)
Contact:
Review: Event Review: Any event affecting this instrument may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date: December 1, 2015
Last Review/Revision: <None>
Changes: